

## Programowanie 2009

Lista zadań nr 13

Na zajęcia 2–3 czerwca 2009

### Grupy zasadnicze

W pierwszych sześciu zadaniach rozważamy algebrę termów pierwszego rzędu.

**Zadanie 1 (1 pkt).** Niech  $\theta_1 \leq \theta_2$  jeśli istnieje takie podstawienie  $\rho$ , że  $\theta_1\rho = \theta_2$ . Niech  $\theta_1 \sim \theta_2$  jeśli  $\theta_1 \leq \theta_2$  i  $\theta_2 \leq \theta_1$ . Udowodnij, że relacja  $\leq$  na podstawieniach jest częściowym porządkiem, relacja  $\sim$  jest relacją równoważności oraz że relacja  $\leq$  na klasach równoważności:

$$[\theta_1]_{\sim} \leq [\theta_2]_{\sim} \iff \theta_1 \leq \theta_2$$

jest poprawnie określona i jest częściowym porządkiem.

**Zadanie 2 (1 pkt).** Mówimy, że term  $s$  jest *ukonkretnieniem* (*konkretyzacją*, *instancją*) termu  $t$  i piszemy  $t \leq s$ , jeżeli istnieje podstawienie  $\theta$ , takie, że  $t\theta = s$ . Mówimy, że termy  $t$  i  $s$  są równoważne i piszemy  $t \sim s$ , jeśli  $t \leq s$  i  $s \leq t$ . Udowodnij, że relacja  $\leq$  na termach jest częściowym porządkiem, relacja  $\sim$  jest relacją równoważności oraz że relacja  $\leq$  na klasach równoważności:

$$[t]_{\sim} \leq [s]_{\sim} \iff t \leq s$$

jest poprawnie określona i jest częściowym porządkiem.

**Zadanie 3 (1 pkt).** Udowodnij, że  $s \sim t$  wtedy i tylko wtedy, gdy termy  $s$  i  $t$  różnią się jedynie nazwami zmiennych, tj. wówczas, gdy istnieje takie podstawienie  $\theta = [x/y_x]_{x \in \text{FV}(s)}$ , że  $y_{x_1} \neq y_{x_2}$  dla  $x_1 \neq x_2$  oraz  $s\theta = t$ .

Niech dane będą dwie różne zmienne  $x$  i  $y$ . Wyznacz zbiór par termów  $\langle t, s \rangle$ , dla których  $[x/t, y/s] = [x/t][y/s]$ . Wyznacz zbiór par termów  $\langle t, s \rangle$ , dla których  $[y/s][x/t] = [x/t][y/s]$ .

**Zadanie 4 (1 pkt).** Niech  $\Gamma = \{t_n \stackrel{?}{=} s_n\}_{n \in \mathbb{N}}$ , gdzie  $t_n, s_n \in \mathcal{T}(\Sigma, \mathcal{X})$ . Pokaż, że jeżeli  $|\mathcal{X}| < \infty$ , to istnieje unifikator  $\Gamma$  wtedy i tylko wtedy, gdy istnieje unifikator każdego skończonego podzbioru  $\Gamma$ . Pokaż, że założenie o skończoności zbioru zmiennych jest istotne.

## Programming 2009

Problem set no. 13

Due June 3, 2009

### Basic groups

In the first six problems we investigate the algebra of first order terms.

**Problem 1 (1 p).** Let  $\theta_1 \leq \theta_2$  if there exists such a substitution  $\rho$  that  $\theta_1\rho = \theta_2$ . Let  $\theta_1 \sim \theta_2$  if  $\theta_1 \leq \theta_2$  and  $\theta_2 \leq \theta_1$ . Prove that the relation  $\leq$  defined on substitutions is a partial preorder, the relation  $\sim$  is an equivalence relation, and a relation  $\leq$  defined on equivalence classes:

$$[\theta_1]_{\sim} \leq [\theta_2]_{\sim} \iff \theta_1 \leq \theta_2$$

is well defined and is a partial order.

**Problem 2 (1 p).** We say that a term  $s$  is an *instance* of a term  $t$  and write  $t \leq s$  if there exist such a substitution  $\theta$ , that  $t\theta = s$ . We say that terms  $t$  and  $s$  are equivalent and write  $t \sim s$  if  $t \leq s$  and  $s \leq t$ . Prove that the relation  $\leq$  defined on terms is a partial preorder, the relation  $\sim$  is an equivalence relation, and a relation  $\leq$  defined on equivalence classes:

$$[t]_{\sim} \leq [s]_{\sim} \iff t \leq s$$

is well defined and is a partial order.

**Problem 3 (1 p).** Prove that  $s \sim t$  if and only if terms  $s$  and  $t$  differ only in names of variables, *i.e.*, when there exists such a substitution  $\theta = [x/y_x]_{x \in \text{FV}(s)}$  that  $y_{x_1} \neq y_{x_2}$  for  $x_1 \neq x_2$  and  $s\theta = t$ .

Let two different variables  $x$  and  $y$  be given. Determine the set of pairs of terms  $\langle t, s \rangle$ , for which  $[x/t, y/s] = [x/t][y/s]$ . Determine the set of such pairs of terms  $\langle t, s \rangle$ , for which  $[y/s][x/t] = [x/t][y/s]$ .

**Problem 4 (1 p).** Let  $\Gamma = \{t_n \stackrel{?}{=} s_n\}_{n \in \mathbb{N}}$ , where  $t_n, s_n \in \mathcal{T}(\Sigma, \mathcal{X})$ . Show that if  $|\mathcal{X}| < \infty$ , then there exists a unifier of  $\Gamma$  if and only if there exists a unifier of every finite subset of  $\Gamma$ . Show that the assumption about finiteness of  $\mathcal{X}$  is essential.

**Zadanie 5 (1 pkt).** Przez *rozmiar termu* będziemy rozumieć liczbę wystąpień symboli funkcyjnych i zmiennych w tym termie. *Rozmiarem równania*  $t \stackrel{?}{=} s$  nazwiemy sumę rozmiarów termów  $t$  i  $s$ , zaś *rozmiarem podstawienia*  $[x_i/t_i]_{i=1}^n$  nazwiemy sumę rozmiarów termów  $t_i$ . Pokaż, że istnieje równanie  $t \stackrel{?}{=} s$  rozmiaru  $n$ , którego najogólniejszy unifikator ma rozmiar  $2^{\Omega(n)}$ .

**Zadanie 6 (1 pkt).** Niech  $\Sigma$  będzie sygnaturą jednogatunkową, zaś  $\mathcal{X}$  zbiorem zmiennych. Rozważmy dwa rodzaje par termów: *równości*, zapisywane w postaci  $s = s'$  i *nierówności*, zapisywane w postaci  $t \neq t'$ . *Rozwiązaniem* zadania

$$\{s_i = s'_i\}_{i=1}^n \cup \{t_j \neq t'_j\}_{j=1}^m$$

jest takie podstawienie  $\theta$ , że  $s_i\theta = s'_i\theta$  dla  $i = 1, \dots, n$  oraz  $t_j\theta \neq t'_j\theta$  dla  $j = 1, \dots, m$ . Niech  $\mathcal{R}$  będzie zbiorem rozwiązań powyższego zadania. Pokaż, że jeżeli  $\mathcal{R} \neq \emptyset$ , to istnieje w  $\mathcal{R}$  rozwiązanie najbardziej ogólne, tj. istnieje takie  $\theta_0 \in \mathcal{R}$ , że dla każdego  $\theta \in \mathcal{R}$  zachodzi  $\theta_0 \leq \theta$ . Podaj przykład ilustrujący, iż — w odróżnieniu od zwykłej unifikacji — jeśli  $\theta_0 \in \mathcal{R}$  jest najbardziej ogólnym rozwiązaniem, to istnieją podstawienia  $\theta \geq \theta_0$ , które nie należą do  $\mathcal{R}$ .

Opisz algorytm znajdowania najogólniejszego rozwiązania powyższego zadania i uzasadnij, że jest on poprawny.

W kolejnych zadaniach rozważamy rachunek lambda z typami prostymi zadany regułami:

$$\begin{aligned} t &::= x \mid t_1 t_2 \mid \lambda x. t \\ \sigma &::= \alpha \mid \sigma_1 \rightarrow \sigma_2 \end{aligned}$$

$$\frac{}{\Gamma, x : \sigma \vdash x : \sigma} \quad \frac{\Gamma \vdash t_1 : \sigma_2 \rightarrow \sigma_1 \quad \Gamma \vdash t_2 : \sigma_2}{\Gamma \vdash t_1 t_2 : \sigma_1} \quad \frac{\Gamma, x : \sigma_1 \vdash t : \sigma_2}{\Gamma \vdash \lambda x. t : \sigma_1 \rightarrow \sigma_2}$$

**Zadanie 7 (1 pkt).** Wskaż, które wyrażenia posiadają typ. Wyznacz ich typy główne i napisz dowody używając reguł typowania. Uzasadnij dlaczego pozostałe wyrażenia nie mają typu.

1.  $\lambda xy. x$
2.  $\lambda xy. y$
3.  $\lambda xy. xx$
4.  $\lambda xy. yx$
5.  $\lambda xy. xyx$
6.  $\lambda xy. yxx$
7.  $\lambda xy. x(yx)$
8.  $\lambda xy. y(yx)$
9.  $\lambda xy. yxxx$
10.  $\lambda xy. y(xy)x$
11.  $\lambda xy. y(yx)x$

12.  $\lambda xy. xy(yx)$
13.  $\lambda xy. yx(yx)$
14.  $\lambda xy. x(yxx)$
15.  $\lambda xy. y(yxx)$
16.  $\lambda xy. x(x(yx))$
17.  $\lambda xy. x(y(yx))$
18.  $\lambda xy. y(y(xx))$
19.  $\lambda xy. y(y(yx))$
20.  $\lambda xy. xyxyyy$
21.  $\lambda xy. x(xy)(xy)$
22.  $\lambda xy. x(xy)(yx)$

**Problem 5 (1 p).** The *size of a term* is the number of occurrences of function symbols and variables in it. The *size of an equation*  $t \stackrel{?}{=} s$  is the sum of the sizes of terms  $t$  and  $s$ , and the *size of a substitution*  $[x_i/t_i]_{i=1}^n$  is the sum of the sizes of terms  $t_i$ . Show that there exists an equation  $t \stackrel{?}{=} s$  of size  $n$  whose most general unifier has size  $2^{\Omega(n)}$ .

**Problem 6 (1 p).** Let  $\Sigma$  be a single-sorted signature, and  $\mathcal{X}$  — a set of variables. We consider two kinds of pairs of terms: *equalities* written  $s = s'$ , and *inequalities* written  $t \neq t'$ . A *solution* of a problem

is such a substitution  $\theta$ , that  $s_i\theta = s'_i\theta$  for  $i = 1, \dots, n$ , and  $t_j\theta \neq t'_j\theta$  for  $j = 1, \dots, m$ . Let  $\mathcal{R}$  be a set of solutions of the problem above. Show that if  $\mathcal{R} \neq \emptyset$ , then there exists in  $\mathcal{R}$  the most general solution, i.e., there exists such  $\theta_0 \in \mathcal{R}$ , that for any  $\theta \in \mathcal{R}$  one has  $\theta_0 \leq \theta$ . Give an example that — contrary to the ordinary unification — if  $\theta_0 \in \mathcal{R}$  is the most general unifier, then there exist substitutions  $\theta \geq \theta_0$  that do not belong to  $\mathcal{R}$ .

Describe an algorithm for finding the most general solution of the problem above and prove its correctness.

In the following problems we consider the simply typed lambda calculus given by the rules:

**Problem 7 (1 p).** Indicate which terms are typable. Determine their principal types and write proofs using the inference rules. Give arguments why remaining terms are not typable.

23.  $\lambda xy. x(yx)(xy)$
24.  $\lambda xy. x(yx)(yx)$
25.  $\lambda xy. x(yx(xy))$
26.  $\lambda xy. x(yx(yx))$
27.  $\lambda xy. x(yxxx)$
28.  $\lambda xy. y(yxxx)$
29.  $\lambda xy. x(y(xy)x)$
30.  $\lambda xy. x(y(yx)x)$
31.  $\lambda xy. x(x(xy)y)$
32.  $\lambda xy. x(x(yxx))$
33.  $\lambda xy. x(y(yxx))$
34.  $\lambda xy. x(x(x(xy)))$
35.  $\lambda xy. x(x(x(yx)))$
36.  $\lambda xy. x(x(y(xy)))$
37.  $\lambda xy. xy(yxx)$
38.  $\lambda xy. xy(x(xy))$
39.  $\lambda xy. xy(x(yx))$
40.  $\lambda xy. yx(x(yx))$
41.  $\lambda x. x(x(\lambda y. x))$
42.  $\lambda x. x(\lambda y. x(\lambda z. z))$
43.  $\lambda x. x(\lambda y. yxx)$
44.  $\lambda x. x(\lambda y. y(\lambda z. x))$

**Zadanie 8 (1 pkt).** (Pokaż mi swój typ, a powiem ci, kim jesteś.) Niech  $t$  będzie takim termem w postaci  $\beta$ -normalnej, że

$$\vdash t : \alpha \rightarrow \beta \rightarrow \alpha.$$

Udowodnij, że  $t = \lambda xy.x$ .

**Problem 8 (1 p).** (Show me your type and I'll tell you who you are.) Let  $t$  be such a term in  $\beta$ -normal form that

Prove that  $t = \lambda xy.x$ .

## Grupy rozszerzone

**Zadanie 1 (1 pkt).** Udowodnij, że jeśli  $\Gamma \vdash t : \sigma$ , to  $\text{FV}(t) \supseteq \text{Dom}(\Gamma)$ . Udowodnij, że jeśli  $\Gamma_1 \vdash t : \sigma$  i  $\Gamma_1 \upharpoonright \text{FV}(t) = \Gamma_2 \upharpoonright \text{FV}(t)$ , to  $\Gamma_2 \vdash t : \sigma$ .

**Zadanie 2 (1 pkt).** Udowodnij, że jeżeli  $\Gamma \vdash t : \sigma$  i  $t \xrightarrow{\beta} s$ , to  $\Gamma \vdash s : \sigma$ .

**Zadanie 3 (1 pkt).** Pokaż, że twierdzenie odwrotne do rozważanego w poprzednim zadaniu nie zachodzi, tj. z tego, że  $t \xrightarrow{\beta} s$  i  $s$  posiada typowanie nie wynika, że typowanie posiada  $t$ . Niech  $\Gamma \vdash t : \sigma$  będzie typowaniem głównym  $t$ ,  $t \xrightarrow{\beta} s$  i  $\Gamma' \vdash s : \sigma'$  będzie typowaniem głównym  $s$ . Jaka zależność zachodzi między  $(\Gamma, \sigma)$  i  $(\Gamma', \sigma')$ ?

**Zadanie 4 (1 pkt).** Udowodnij, że jeśli  $\vdash t : \sigma$ , to typ  $\sigma$  rozumiany jako formuła rachunku zdań w której zmienne typowe oznaczają zmienne zdaniowe a „ $\rightarrow$ ” oznacza implikację jest tautologią.

**Zadanie 5 (1 pkt).** Pokaż, że istnieje wyrażenie rozmiaru  $n$ , którego typ główny ma rozmiar  $2^{\Omega(n)}$  (wzoruj się na podobnym przykładzie dla zadania unifikacji). Pokaż, że typ główny wyrażenia rozmiaru  $n$  ma rozmiar  $2^{O(n)}$ .

**Zadanie 6 (1 pkt).** Typ jest *niepusty*, jeśli istnieje zamknięte wyrażenie tego typu. Wśród typów podanych poniżej wskaż typy niepuste. Dla każdego z nich podaj przykład zamkniętego wyrażenia, dla którego jest on typem głównym. Dla pozostałych typów uzasadnij, dlaczego są puste.

1.  $\alpha \rightarrow \alpha$

2.  $\alpha \rightarrow \alpha \rightarrow \alpha$

3.  $\alpha \rightarrow \beta \rightarrow \alpha$

4.  $\alpha \rightarrow \beta \rightarrow \beta$

5.  $(\alpha \rightarrow \beta) \rightarrow \alpha$

6.  $\alpha \rightarrow \alpha \rightarrow \alpha \rightarrow \alpha$

7.  $\alpha \rightarrow \alpha \rightarrow \alpha \rightarrow \beta$

8.  $\alpha \rightarrow \alpha \rightarrow \beta \rightarrow \alpha$

9.  $\alpha \rightarrow (\alpha \rightarrow \alpha) \rightarrow \alpha$

10.  $\alpha \rightarrow (\alpha \rightarrow \beta) \rightarrow \alpha$

11.  $\alpha \rightarrow (\alpha \rightarrow \beta) \rightarrow \beta$

12.  $\alpha \rightarrow (\beta \rightarrow \alpha) \rightarrow \alpha$

13.  $\alpha \rightarrow (\beta \rightarrow \alpha) \rightarrow \beta$

14.  $(\alpha \rightarrow \alpha) \rightarrow \beta \rightarrow \beta$

15.  $(\alpha \rightarrow \beta) \rightarrow \beta \rightarrow \alpha$

16.  $(\alpha \rightarrow \alpha \rightarrow \alpha) \rightarrow \alpha$

17.  $((\alpha \rightarrow \alpha) \rightarrow \alpha) \rightarrow \alpha$

18.  $((\alpha \rightarrow \alpha) \rightarrow \beta) \rightarrow \beta$

19.  $((\alpha \rightarrow \beta) \rightarrow \alpha) \rightarrow \alpha$

20.  $((\alpha \rightarrow \beta) \rightarrow \beta) \rightarrow \alpha$

**Zadanie 7 (1 pkt).** Niech NF oznacza zbiór termów w postaci  $\beta$ -normalnej. Pokaż, że

$$\{t \in \text{NF} \mid \vdash t : (\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)\} = \{\lambda xy.x^{(n)}y \mid n \in \mathbb{N}\} \cup \{\lambda x.x\}.$$

## Extended groups

**Problem 1 (1 p).** Prove that if  $\Gamma \vdash t : \sigma$ , then  $\text{FV}(t) \supseteq \text{Dom}(\Gamma)$ . Prove that if  $\Gamma_1 \vdash t : \sigma$  and  $\Gamma_1 \upharpoonright \text{FV}(t) = \Gamma_2 \upharpoonright \text{FV}(t)$ , then  $\Gamma_2 \vdash t : \sigma$ .

**Problem 2 (1 p).** Prove that if  $\Gamma \vdash t : \sigma$  and  $t \xrightarrow{\beta} s$ , then  $\Gamma \vdash s : \sigma$ .

**Problem 3 (1 p).** Show that the converse theorem to the one proved in the previous problem does not hold, *i.e.*, the assumptions that  $t \xrightarrow{\beta} s$  and that  $s$  has a typing do not imply that  $t$  has a typing. Let  $\Gamma \vdash t : \sigma$  be a principal typing for  $t$ ,  $t \xrightarrow{\beta} s$  and  $\Gamma' \vdash s : \sigma'$  be a principal typing for  $s$ . How  $(\Gamma, \sigma)$  corresponds to  $(\Gamma', \sigma')$ ?

**Problem 4 (1 p).** Prove that if  $\vdash t : \sigma$ , then the type  $\sigma$  considered as a propositional formula where type variables stand for propositional variables and “ $\rightarrow$ ” is an implication is a tautology.

**Problem 5 (1 p).** Prove that there exists a term of size  $n$  whose principal type has size  $2^{\Omega(n)}$  (follow a similar example for the unification problem). Prove that a principal type of a term of size  $n$  has size  $2^{O(n)}$ .

**Problem 6 (1 p).** A type is *inhabited* if there exists a closed term of that type. Indicate inhabited types among types presented below. For every such type give an example of a closed term for which this type is principal. For remaining types give arguments why they are not inhabited.

**Problem 7 (1 p).** Let NF stands for the set of terms in  $\beta$ -normal form. Show that

Innymi słowy termy typu

In other words terms of type

$$(\alpha \rightarrow \alpha) \rightarrow (\alpha \rightarrow \alpha)$$

to liczebniki Churcha.

are the Church numerals.

**Zadanie 8 (1 pkt).** Udowodnij, że jeśli term posiada typowanie, to posiada też postać normalną. *Wskazówka:* zdefiniuj miarę złożoności termów (zależną od liczby i stopnia komplikacji redexów), uporządkuj ją dobrym porządkiem i opracuj strategię redukcji, która w każdym kroku zmniejsza tę miarę.

**Problem 8 (1 p).** Prove that if a term has a typing, then it has a normal form as well. *Hint:* define a measure of complexity of terms (that depends on the number and degree of complication of redexes), order it by a well founded ordering and devise a reduction strategy which decreases this measure in every step.

## Grupa zaawansowana

## Advanced group

**Zadanie 1 (1 pkt).** Zdefiniuj algorytm działający w czasie liniowym, który dla danego problemu unifikacji tworzy lambda wyrażenie, które posiada typ wtedy i tylko wtedy, gdy dany problem unifikacji posiada rozwiązanie. Na wykładzie opisaliśmy redukcję odwrotną. Zatem problemy unifikacji i typowania są równoważne względem LINTIME-redukcji. Czy potrafisz zdefiniować takie redukcje działające w logarytmicznej pamięci?

**Problem 1 (1 p).** Define an algorithm running in linear time that for a given instance of the unification problem creates a lambda term that is typable if and only if the given unification problem has a solution. During the lecture we described a reduction in the opposite direction. Thus the unification and typing problems are LINTIME-equivalent. Can you define such reductions running in a logarithmic space?

**Zadanie 2 (2 pkt).** Udowodnij, że jeśli term posiada typowanie, to jest mocno normalizowalny.

**Problem 2 (2 p).** Prove that if a term has a typing, then it is strongly normalizing.

**Zadanie 3 (1 pkt).** Wskaż tautologię klasycznego rachunku zdań będącą pustym typem.

**Problem 3 (1 p).** Produce a tautology of the classical propositional calculus which is not inhabited as a type.

**Zadanie 4 (2 pkt).** Opisz algorytm, który dla podanego typu odpowiada na pytanie, czy typ ten jest niepusty. *Uwaga:* odkrywanie tautologii klasycznego rachunku zdań jest co-NP-zupełne. Ten problem jest jeszcze trudniejszy: odkrywanie typów niepustych jest PSPACE-zupełne.

**Problem 4 (2 p).** Describe an algorithm which for a given type decides if this type is inhabited. *Remark:* discovering tautologies of the classical propositional calculus is co-NP-complete. This problem is even harder: discovering inhabited types is PSPACE-complete.

**Zadanie 5 (2 pkt).** Czy istnieje taki typ niepusty, że dla każdego zamkniętego termu nie jest on jego typem głównym? Czy istnieje taki typ niepusty, że dla każdego zamkniętego termu w postaci normalnej nie jest on jego typem głównym?

**Problem 5 (2 p).** Does there exist such an inhabited type, that it is not a principal type for any closed term? Does there exist such an inhabited type, that it is not a principal type for any closed term in normal form?